Original Research Paper Engineering

Detection and Removal of Wormhole Attacker Node in MANET using Multi Path Algorithm

Geetika Srivastava M.Tech. Scholar, Department of Electronics and Communication, IES College of Technology, Bhopal

Sonu Lal Assistant Professor, Department of Electronics and Communication, IES College of Technology, Bhopal

ABSTRACT

MANET is a wireless network so more security is needed here. MANET is susceptible to several attacks, including a major attack known as the wormhole attack. This is a very powerful attack, and prevention is very difficult. In this attack, malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route. If source node chooses this false route, malicious nodes have the option of delivering the packets or dropping them. In this paper we are considering detection and blacklisting of Wormhole attacker node present in MANET. In this paper we are going to detect malicious nodes, using a hop-count and time delay analysis from the user's point of view without considering special environment assumptions. The proposed work is simulated using OPNET modeler and result signifies the advantages of proposed work.

KEYWORDS : Mobile ad hoc network (MANET), hop-count analysis and time delay, security, wormhole attack.

INTRODUCTION

The Mobile Ad-hoc Network (MANET) self organized network with no fixed infrastructure. It has dynamic topology and fast deployment facility. MANET is extremely vulnerable to attacks due to dynamic topology. In MANET each node is capable to act as source destination and router. Hence, each node has the ability to communicate directly with another node.

In figure 1 scenario of wormhole attack is there. Node with black color is source and destination. Node with blue color is route node and node with orange color is wormhole attacker node.

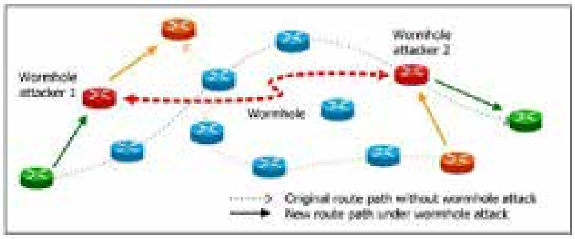

Wormhole attacker 1
Wormhole attacker 2
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Fig 1 the wormhole attack in MANET

It is supposed that the packets will go from source to destination via route nodes (blue nodes). But in fig 1 it is shown that wormhole attacker node is bypassing the route nodes. This is not at all desirable. Practically this wormhole node represents hacker or attacker of the MANET. So it is required to detect and blacklist these types of nodes so that this will not happen in future. We are going to detect the attack based upon Hope count and time delay. If any one of or both of them decreases abruptly then it is supposed that attack took place. Then the process starts to detect and blacklisting the attacker node.

PROPOSED ANALYSIS MODUE

The proposed research methodology is cited below

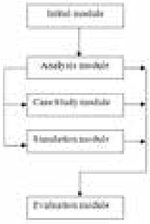


Fig 2 Research Methodology

In this first step is to find out the problem. Then that has to be analyzed. After this different cases are considered related to this. After analysis based upon analyzed result simulation is carried out. After this last step is to evaluate the proposed method.

LITERATURE SURVEY

This section, we are going to get idea about the developments regarding wormhole attack and its remedy what has developed yet.

Packet Leash [2] geographic leash and temporal leash are the type of packet leashes. This is an approach towards transmission of data packets up to longer distances. In geographic leash, when a node A sends a packet to another node B, the node must include its sending time and location information the packet. B is to estimate the distance between A and B. The geographic leash computes an upper bound of the distance, but the temporal leash confirms that a packet has upper bound of its lifetime.

Shalini Jain et al. [4] provides a great approach in identifying and isolating nodes that create a wormhole attack in the MANET without engaging cryptographic measures.

Sun Choi et al. [5] provide a substantive method named WAP without using perquisite hardware. WAP works on the basis of RERQ (Route Request) and RERP (Route Reply).

Most of the above explained techniques require special assumptions and supporting hardware, and some of them are strictly based on specific protocols only.

PROPOSED WORK

In this proposed work we are considering Wormhole attack only because it does not need exploiting any other nodes of the network but it interferes with the route establishment process. We are going to implement a newer method which is going to detect the wormhole attacker node and it will work without modification of AODV algorithm, using average hop-count as well as average time delay analysis. The proposed work is going to be simulated using OPNET modeler 14.0. The various steps of modeling in FSM (Finite State Machine) of this Proposed Algorithm are as follows:

Step1. Randomly estimate a number from least to maximum number of nodes.

Step2. Make this Node with same number as the transmitter node.

Step3. Find the feasible Route from selected transmitting node to any destination node with specified average route.

Step4. Transmit this packet as per selected destination and let the timer start to count total hops and total delay.

Step5. Store all routes and their respective hops count and delay by repeating this process.

Step6. If the hop count for a particular route is found decreased abruptly for average hop count then at least one attacker node must be present in that route.

Step7. Now the delay of all previous routes are checked which may have any node of the suspicious route.

Node not encounter previously may be malicious let there are N such nodes.

Step8. If N == 1 then it is the attacker. Else wait for future sequences which signify the deviation which involves only one of N nodes.

Step9. These nodes are made black listed and they are not involved in any of the future routes.

Step10. Step1 to step9 is repeated until the specified target. Target may be

1. To run for specific number of packets etc.
2. To run for specified time.
3. To get complete list of malicious nodes.

IMPLEMENTATION AND RESULTS

The verification of proposed algorithm is done on the basis major analysis parameters for which scenarios configured as:

1. Algorithm works with High (50) Nodes density with varying number of attacker nodes.
2. Effect of algorithm under several t traffic conditions.

SIMULATION ENVIRONMENT AND PARAMETERS

Proposed algorithm is justified only with OPNET network modeler14.0 the radio model corresponds to the 802.11 Wireless LAN, operating at a maximum rate of 11 Mbps. CBR traffic pattern is tested.

PARAMETERS

No. of nodes	50
Area	9 square KM
No. of Malicious Nodes	6
Packet Interval Time	3 sec const.
Traffic Model	CBR
Data Rate	11 Mbps
Routing Protocol	AODV
MAC	Random
Packet Size	1024 bits(approx)

RF TRANCEIVER PROPERTIES

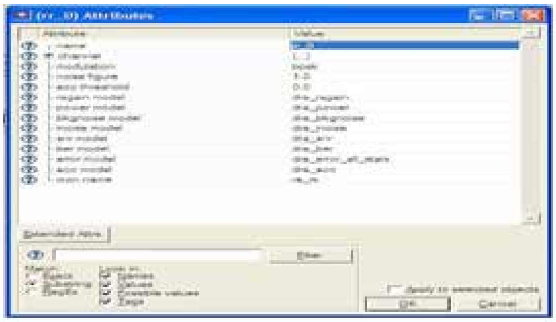


Fig 3 Transmitter and receiver

SIMUATION RESULTS

The simulation results from OPNET Modeler 14.0 with respect to the Average Hop count per route and Average delay per route in different scenario**.**

Scenario 1:- 50 Nodes distribution without wormhole attack:

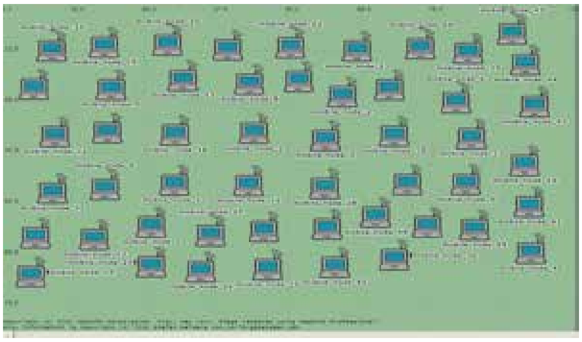
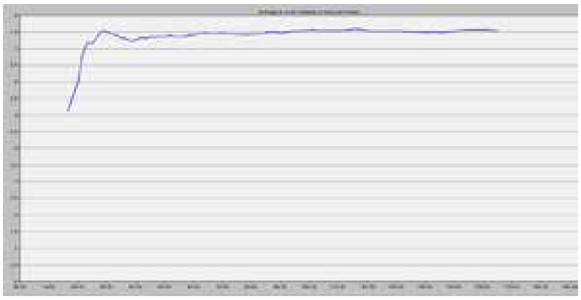


Fig 4

This distribution in this scenario is for high node density system with no wormhole attack. Distribution is supposed to be uniform. Each node in this can act as transmitter, receiver and router. As this are the basic properties of MANET. Each node is having transmitting and receiving antenna.

Average Hop count and average time delay per route in scenario 1 without wormhole attack



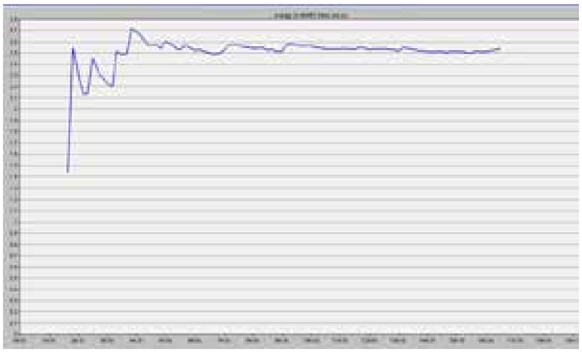


Fig 5

From this average delay per route will be used as reference for attack indicator. In this scenario this delay is found to be 2.2.

Scenario 2:- 50 Nodes distribution with wormhole attack

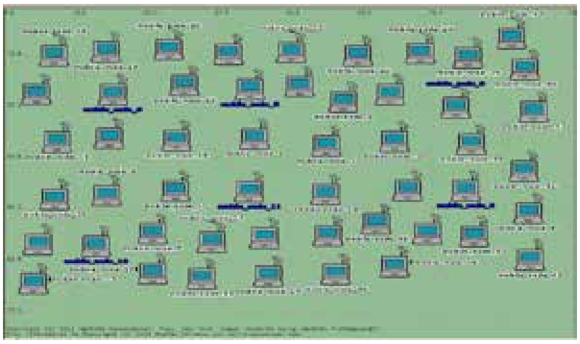


Fig 6

With uniform node distribution this scenario is for with wormhole attack. Attacking tunnel is highlited in this figure.

Average Hop count per route in scenario 2 with wormhole attack

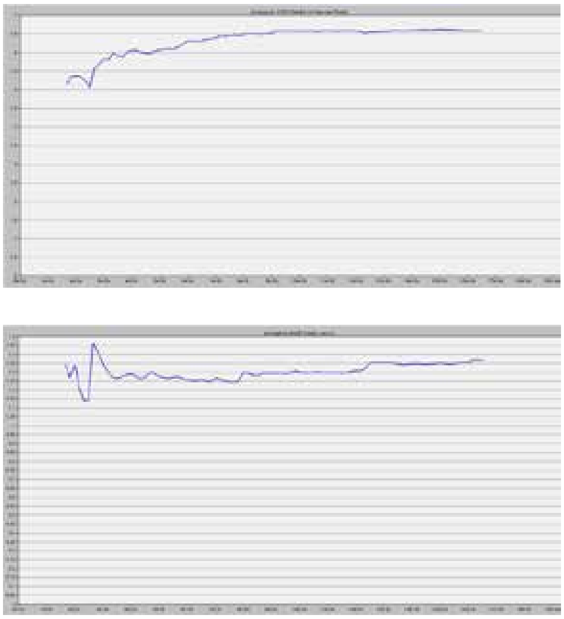


Fig 7

In Present scenario Average hop count per route decrease from 7.3 to 6.2.

Scenario 3:- 50 Nodes distribution with wormhole attack and applied proposed Algorithm

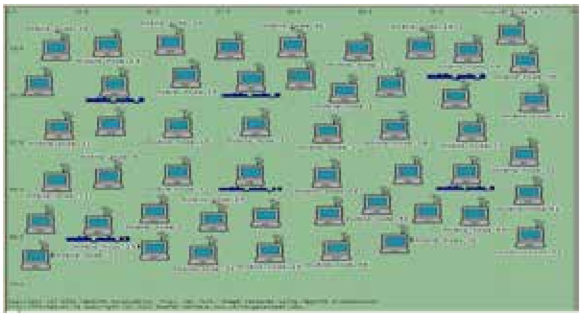
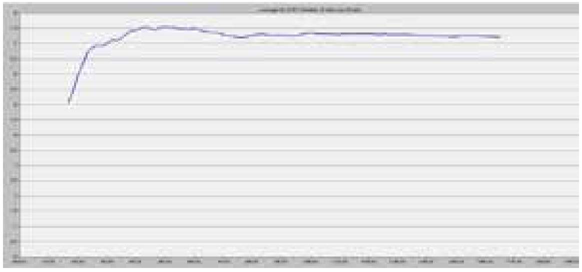


Fig 8

After proposed algorithm this scenario having attacking tunnel between highlited nodes.

Average Hop count per route in scenario 3 with wormhole attack and applied proposed Algorithm



Initial distribution of the nodes which is almost uniform this scenario is for high node density system with wormhole attack. The scenario having an attacking tunnel between highlighted nodes, and applied proposed algorithm of them.

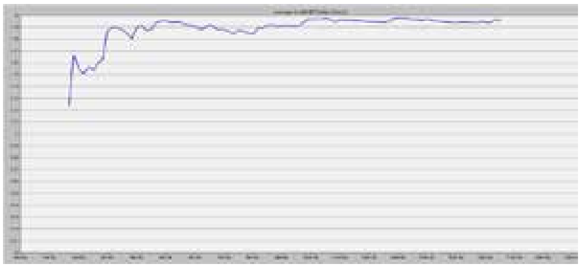


Fig 9

Average hope count and average delay in scenario 3 is almost equal to the situation when no attack was there.

Average Hop count and time delay per route comparison in 50 nodes

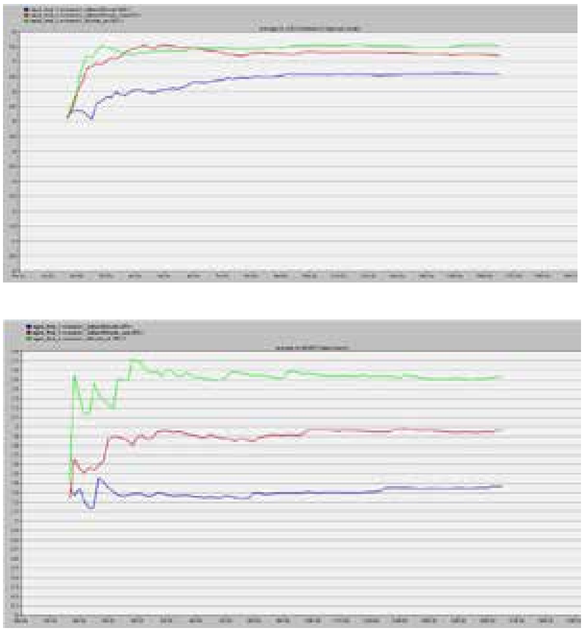


Fig 10

From the above plots conclusions regarding proposed algorithm can easily be understood. It is evident that hop count is reduced by 12%

(blue color line) from initial condition (green color line) this represents the effectiveness of proposed algorithm.

Average delay is reduced by 49% (blue color line) from normal condition (green color line). This represents reduction of route by attacking route. The proposed algorithm has better delay which signifies the elimination of attacker node.

CONSLUSION

Thus this proposed method using hope count and time delay analysis gives good performance in detecting and blacklisting the wormhole attacker node in MANET. Also, this method works without modification of algorithm.

When the malicious node is found then immediately this node is blacklisted by the source node so next nodes are not involved in this. This method also provides good performance for high node density MANET network compare to average and low density network.

REFERENCES

1. Khabbazian, M.; Mercier, H.; Bhargava, V.K. Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks. IEEE Trans. Wireless Commun. 2009, 8, 736–745
2. D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors,Mobile Computing, volume 353, pages 153–181. Kluwer Academic Publishers, 1996.
3. D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. RFC 4728, The Internet Engineering Task Force, Network Working Group, Feb 2007. http://www.ietf.org/rfc/rfc4728.txt
4. Ali Ghaffari , " Vulnerability and Security of Mobile Ad hoc Networks ", in Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006, pp.124-129